UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/549,408	09/14/2005	Junbiao Zhang	PU030081	1829

24498 7590 08/07/2008

Joseph J. Laks
Thomson Licensing LLC
2 Independence Way, Patent Operations
PO Box 5312
PRINCETON, NJ 08543

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
08/07/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/549,408	ZHANG ET AL.	
	Examiner	Art Unit	
	SYED ZIA	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 April 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to remarks filed on April 28, 2008. Original application contained Claims 1-24. Applicant currently amended Claims 5-8, 11, 12-24, and 17. Therefore, Claims 1-24 are pending for further consideration.

Response to Arguments

Applicant's arguments filed on April 28, 2008 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1-24 applicants argued that the cited prior arts (CPA) [Stenman et al. (EP 1178644 A2)] do not teach, "*periodically generating a subsequent session key, and logoff message in encrypted form and including the secure key*".

This is not found persuasive. The system of cited prior art teaches a method for providing security key management method for wireless local area network which involves generating IPsec authentication, encryption and decryption keys using certificates and private key for packets transferred between mobile terminal and server.

In cited prior art, when the mobile terminal first associates with a respective access point in the network, it uses the IKE with private key and the certificates to generate the wireless local area network link level keys with that access point. Mutual authentication of both the mobile terminal and access point is achieved by this process. When end-to-end IPsec security is

employed, the mobile terminal uses the IKE to generate the authentication keys and ciphering keys with the network server. When transmitting packets, the IPsec kernel in the mobile terminal generates the Authentication Header (AH) and encrypts the packets. In the server, the packets are authenticated and decrypted. Link level session keys are used to encrypt traffic over the shared frequency and air space.

Thus in cited prior art, the certificates are obtained from a certificate authority and a private key are used with Internet key exchange to generate a wireless local area network link level, and the mobile terminal and the access point are mutually authenticated. The keys are used to generate IPsec authentication, encryption and decryption keys for data packets transferred between the mobile terminal and the server.

As a result, the system of cited prior art does implement and teaches a system and method that relates to wireless local area network secure session management (summary, Fig.1-5, and col.5 line 44 to col.8 line 48).

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that cited prior art does teach or suggest the subject matter broadly recited in independent Claims and in subsequent dependent Claims. Accordingly, rejections for claims 1-24 are respectfully maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-24 are rejected under 35 U.S.C. 102(a) as being anticipated by Stenman et al. (EP 1178644 A2).

1. Regarding Claim 1 Stenman teach and describe a method for providing a secure communications session with a user terminal in a communications network (Fig.3-5), the method comprising the steps of: transmitting first and second secure keys to the user terminal using a secure communications method, the first and second secure keys being suitable for storage in the user terminal for use during the secure communications session; encrypting and transmitting data to the user terminal using a current session key, and receiving and decrypting data received from the user terminal using the current session key, the first secure key initially being used as the current session key; and periodically generating by an access point a subsequent session key using the second secure key and using the subsequent session key as the current session key during subsequent communications between the communications network and the user terminal (col.5 line 44 to col.8 line 48).

2. Regarding Claim 4 Stenman teach and describe a method for providing a secure communications session with a mobile terminal in a wireless local access network, the method comprising the steps of: transmitting first and second secure keys to the mobile terminal using a secure communications method, the first and second secure keys being suitable for storage in tile mobile terminal for use during the secure communications session; encrypting and transmitting data to the mobile terminal using a current session key, and receiving and decrypting data received from the mobile terminal using the current session key, the first secure key initially being used as the current session key; and periodically generating a subsequent session key using the second secure key and using the subsequent session key as the current session key during subsequent communications with the mobile terminal (col.5 line 44 to col.8 line 48).

3. Regarding Claim 7 Stenman teach and describe a method for providing a secure communications session with a mobile terminal in a wireless local access network, the method comprising the steps of: generating a secure key; transmitting the secure key to the mobile terminal using a secure communications method, the secure key being stored in the mobile terminal for use during the secure communications session; encrypting and transmitting data to the mobile terminal using a current session key, and receiving and decrypting data received from the mobile terminal using the current session key; and ending the secure communications session by an access point in response to receiving a logoff message from the mobile terminal, the logoff message being in encrypted form and including the secure key (col.5 line 44 to col.8 line 48).

4. Regarding Claim 8 Stenman teach and describe a method for providing a secure communications session with a mobile terminal in a wireless local access network the method comprising the steps of: generating first and second secure keys; transmitting the first and second secure keys to the wireless local area network using a secure communications method, the first and second secure keys being stored in the wireless local area network or use during the secure communications session; encrypting and transmitting data to the wireless local area network using a current session key, and receiving and decrypting data received from the wireless local area network using the current session key, the first secure key initially being used as the current session key; and periodically generating by the mobile terminal a subsequent session key using the second secure key and using the subsequent session key as the current session key during subsequent communications with the wireless local area network (col.5 line 44 to col.8 line 48).

5. Regarding Claim 11 Stenman teach and describe a method for providing a secure communications session with a mobile terminal in a wireless local access network, the method comprising the steps of: generating a secure key; transmitting the secure key to the wireless local area network using a secure communications method, the secure key being stored in the wireless local area network for use during the secure communications session; encrypting and transmitting data to the wireless local area network using a current session key, and receiving and decrypting data received from the wireless local area network using the current session key; and ending the secure communications session in response to receiving a logoff message from the wireless local area network, the logoff message being in encrypted form and including the secure key(col.5 line 44 to col.8 line 48).

6. Regarding Claim 12 Stenman teach and describe a method for providing a secure communications session with a mobile terminal in a wireless local access network, the method comprising the steps of: installing at least two shared secrets on both the mobile terminal and the wireless local area network access point during the user- authentication phase whereby a first secret is the initial session key and a second secret is utilized as secure seed to generate subsequent session keys (col.5 line 44 to col.8 line 48).

7. Regarding Claim 18 Stenman teach and describe a method for providing a secure communications session between a mobile terminal and a wireless local access network, the method comprising the steps of: a mobile terminal sending during session logoff an encrypted logoff request accompanied by the secure seed such that the secure seed appears in the logoff request (col.5 line 44 to col.8 line 48).

8. Regarding Claim 19 Stenman teach and describe an access point for providing a secure communications session between a mobile terminal and a wireless local access network, comprising: a means for transmitting first and second secure keys to the mobile terminal using a secure communications method and a means to encrypt data using the first secure .key and a means to periodically generate a subsequent session key using the second secure key (col.5 line 44 to col.8 line 48).

9. Regarding Claim 20 Stenman teach and describe a terminal device for providing a secure communications session with a communications network, comprising:
a means to receive a secure key and a secure seed and a means to store the secure key and the secure seed for use during the secure communications session; a means to receive data and a means to decrypt the data using a current session key during the secure communications session, the secure key being using initially as the current session key; and a means to generate a subsequent session key using the current session key and the secure seed, the subsequent session key thereafter being used as the current session key for subsequent communications (col.5 line 44 to col.8 line 48).

10. Regarding Claim 24, Stenman teach and describe an access point for providing a secure communications session between a mobile terminal and a wireless local area network, comprising: a means to transmit a secure key and a secure seed and a means to store the secure key and the secure seed for use during the secure communications session;
a means to encrypt data and a means to transmit data to the mobile terminal and a means to receive data and a means to decrypt the data from the mobile terminal using a current session key during the secure communications session, the secure key being using initially as the current session key; and a means to generate a subsequent session key using the current session key and the secure seed, the subsequent session key thereafter being used as the current session key for subsequent communications (col.5 line 44 to col.8 line 48)

10. Claims 2-3, 5-6, 9-10, 13-7, and 21-23 are rejected applied as above rejecting Claims 1, 4, 8, 12, and 20. Furthermore, Stenman teach and describe a method for providing a secure communications session between a mobile terminal and a wireless local access network, wherein:

- logging off the user terminal in response to an encrypted logoff request from the user terminal accompanied by the second secure key, and periodically generating step comprises generating the access point a subsequent session key by concatenating the current session key with the second secure key and applying a hash algorithm (col.5 line 17 to col.6 line 41).

the periodically generating step comprises generating the access point a subsequent session key: by concatenating the new key and the second secure key and running a hash algorithm to generate the subsequent session key, and by using a combination of a new key and the second secure key, the new key being generated using the first secure key (col.5 line 17 to col.6 line 41).

the periodically generating step comprises generating a subsequent session key by concatenating the new key and the second secure key and running a hash algorithm to generate the subsequent session key (col.5 line 17 to col.6line 41).

the step of generating a new key and encrypting the new key with the current session key and exchanging and the new key between the wireless local area network and the mobile terminal key (col.5 line 17 to col.6line 41).

the step of the wireless local area network and the mobile terminal generating a new session key employing the new session key and the secure seed, generating the new session key generation comprises the step of concatenating the said new key to the secure seed, the

step of generating a new session key by applying a hash algorithm on said concatenated result, and the step of using the said new session key in communication between the wireless local area network and mobile terminal key (col.5 line 17 to col.6 line 41).

the terminal device comprises a mobile terminal and the communications network comprises a wireless local area network (Fig.1, 5).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
August 01, 2008
/Syed Zia/
Primary Examiner, Art Unit 2131